Protection method against copying of computer software

Patent number:	DE19602804
Publication date:	1997-07-31
Inventor:	
Applicant:	HARRAS ROLAND (DE)
Classification:	
- international:	G11B23/28; G06F12/14
- european:	G06F1/00N7R, G11B20/00P, G11B23/28
Application number:	DE19961002804 19960126
Priority number(s):	DE19961002804 19960126

Abstract of **DE19602804**

The protection system used to prevent copying of software involves the generation of a physical defect or change on the storage system, such as the disc or CD-ROM. The data is analysed and the result is documented and stored. When the data is installed for use, it allows a comparison to be made with a similar analysis made of the disc being used. This identifies if the installation disc in authentic or not, and if not blocks the use.

AL

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 196 02 804 A 1**

(51) Int. Cl.[6]:
G 11 B 23/28
G 06 F 12/14

(21) Aktenzeichen: 196 02 804.3
(22) Anmeldetag: 26. 1. 96
(43) Offenlegungstag: 31. 7. 97

(71) Anmelder:
Harras, Roland, 82031 Grünwald, DE

(72) Erfinder:
Erfinder wird später genannt werden

(56) Entgegenhaltungen:
DE 1 95 10 436 A1

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zum Verhindern der Vervielfältigung von Software (Software-Kopierschutz)

(57) Software (Multi-Media, Video-Filme, Computer-Daten oder -Programme) sind entweder während ihres Gebrauches oder vor Gebrauch relativ leicht zu kopieren. Dies wird von Organisationen genauso wie von Laien genutzt, um illegale Kopien zu erstellen bzw. die jeweilige Software (mehrfach) weiterzugeben. Mit Hilfe der Erfindung werden unerwünschtes Kopieren verhindert bzw. Raubkopien unbrauchbar.
Mit dem erfundenen Verfahren wird ein Datenträger (Lieferant von Software) zunächst in einer bestimmten Region mit nachvollziehbaren kleinen Daten-Einheiten beschrieben und dann in eben dieser Region bewußt beschädigt oder verändert. Die resultierenden Auswirkungen auf die Daten-Einheiten werden analysiert und verbunden mit der zu schützenden Software dokumentiert. Bei späteren Anwendungen der Software kann der entsprechende Datenträger erneut analysiert und das Ergebnis mit dem dokumentierten Ergebnis verglichen werden, um die Echtheit des Datenträgers festzustellen. Eine exakte Rekonstruktion der Beschädigung/Veränderung des Datenträgers, welche auch genau die gleichen Fehler hervorbringen würde, ist nicht möglich.

DE 196 02 804 A 1

DE 196 02 804 A 1

Beschreibung

Gerade in der heutigen Zeit stellen Raubkopien von diverser Software ein großes Problem für die jeweiligen Hersteller und auch dem jeweiligen Vertrieb dar. Dies zeigt sich besonders bei Video, Audio, Computer-Programmen, Daten und Multi-Media. In Anbetracht der momentan bereits entwickelten wieder-beschreibbaren CD's mit hoher Speicherkapazität, MOD's, MD's usw. wird sich das Problem, welches bisher am stärksten bei Disketten und Video-Kassetten vorhanden war/ist, in Zukunft wohl noch weiter verstärken und ausbreiten. Der Schaden ist kaum abschätzbar.

Bisherige Anstrengungen wie bei Computerprogrammen das Abfragen einer Seriennummer oder die Veränderung einer Installationsdiskette bei Installation oder bei Video-Cassetten Signale mit aufzuspielen, die die Kopie unbrauchbar machen, haben fast keine Verbesserung erzielt. Professionelle Organisationen und meist sogar Laien waren trotz allem in der Lage, funktionierende Kopien zu erstellen.

Hier wird die Erfindung mit folgendem — zur Vereinfachung hier auf Computer-Software bezogenem — Verfahren Abhilfe schaffen.

1. Ein Datenträger wird (teilweise) mit extrem kleinen Dateien beschrieben. Die Daten, Anordnung und Bezeichnungen dieser Dateien ist immer gleich und nachvollziehbar. Soll beispielsweise ein Computer-Programm geschützt werden, so könnte dieser Datenträger auch eine der (vielen) Installationsdisketten sein. Bei eher kleinen Programmen (oder wenn der Datenträger eine CD bzw. ein Medium mit ähnlich großer Kapazität ist) könnten die o.g. Dateien auch auf ca. 1/3 des Datenträgers geschrieben werden und auf dem freien 2/3 das Programm selbst untergebracht werden. Es müßte dann jedoch darauf geachtet werden, daß mit der nachfolgenden Beschädigung des Datenträgers, das eigentliche Programm nicht betroffen wird.
2. Jetzt wird der Datenträger in der mit den o.g. Dateien beschriebenen Region absichtlich beschädigt/verändert. Dies könnte durch einen Laser, einem heißen Spitz-Gegenstand, Farbe oder einfach durch einen mit einem Skalpell vollzogenen Kratzer geschehen. Diese Beschädigung(en) und vor allem deren Form, Größe, und Örtlichkeit sollten vom Zufall bestimmt werden. Die Veränderung sollte idealerweise von Hand ausgeführt werden, oder durch eine mit Zufallsgenerator versehenen Maschine erfolgen. Es können auch mehrere Beschädigungen vorgenommen werden. Wichtig ist nur, daß sie ausschließlich in der Region des Datenträgers stattfinden, in der vorher nach Punkt 1) entsprechende Test-Dateien geschrieben wurden. Sollte auf dem Datenträger sonst noch Programme und/oder Daten untergebracht sein/werden, so sollen diese nicht beschädigt werden.
3. Nach all dem wird durch ein Scan-Programm versucht, all die unter 1. geschriebenen Dateien/Daten zu lesen. An den beschädigten Stellen wird es diesbezüglich Probleme geben, oder die Daten verändert/verfälscht wiedergegeben werden. Es entsteht zumeist eine Art von Lesefehler, wie er bei Disketten unter "Read-Error" bekannt ist. Unter "Windows" würde normalerweise das Betriebssystem sogar das Scan-Programm unter Hinweis eines Systemfehlers "Von dem Datenträger kann nicht gelesen werden" abbrechen, was allerdings vom Scan-Programm unterbunden wird.

Die somit festgestellten Auswirkungen der unter Punkt 2) durchgeführten Veränderungen werden erfaßt und festgehalten. Dies wird wie ein Fingerabdruck des Datenträgers fungieren und wie ein solcher von Datenträger zu Datenträger unterschiedlich sein. Diese Identifikation ist ferner nicht kopierbar, da bei einem solchen Versuch der Kopiervorgang abgebrochen würde. Selbst mit speziellen Kopierprogrammen könnte ein Duplikat des Datenträgers nur insoweit angefertigt werden, daß bei all den beschädigten Stellen auf der Kopie dann eine Art 'Leerraum' entstünde. Dieser würde jedoch — bei zukünftigen Scans — keinen der o.g. Lesefehler hervorrufen.

4. Die unter 3. gesammelten und festgehaltenen/dokumentierten Analyse-Ergebnisse werden nun in dem Programm (meist im Hauptprogramm, nicht in der Resource), bzw. in der zu schützenden Software, welche mit dem Datenträger geliefert wird, "versteckt". Sie könnten u. U. auch in einem nicht manipulierbaren Bereich des Datenträgers, am besten verschlüsselt, untergebracht werden. Die größtmögliche Sicherheit erreicht man, wenn das Programm erst nach Einfügen dieser Ergebnisse kompiliert wird. In jedem Fall erreicht man somit, daß genau diese Software mit genau diesem Datenträger verbunden wird. Sie sind quasi auf ewig "verheiratet".
5. Die zu schützende Software enthält ein Test-/Scan-Programm, welches bei jedem Start der Anwendung/Software oder bei jeder Anwendung der Software aktiviert wird. Dieses Test-Programm fordert den Anwender z. B. ca. alle 14 Tage auf, den veränderten Datenträger in das bei der Installation benutzte Laufwerk einzulegen. Es testet dann den Datenträger auf die gleiche Weise wie unter 3. Somit erhält man referenzierbare Informationen, welche mit den unter 4. dokumentierten Daten verglichen werden können.
6. Sollten die Daten außerhalb bestimmter Tolleranzen als nicht übereinstimmend erkannt werden, so ist sichergestellt, daß es sich nicht um den Original-Datenträger handelt. Das Test-Programm könnte dann die jeweilige Software löschen, oder einfach den weiteren Zugriff auf diese Software verweigern.

Der wesentliche Punkt liegt darin, daß die unter 2. durchgeführte Beschädigung/Veränderung des Datenträgers nicht (oder zumindest nur äußerst unwahrscheinlich) exakt reproduziert werden kann. Auch die generelle Chance auf eine genaue Kopie des Datenträgers ist mehr als gering. Denn: Die durch die Beschädigung zerstörten Bereiche des Datenträgers können nicht (oder nur verstümmelt) gelesen werden. Es entsteht ein sog. Lesefehler. Dieser gilt in den meisten Betriebssystemen als Systemfehler und ist softwaremäßig oder mit einer Kopiervorrichtung nicht reproduzierbar. Es wird wahrscheinlich sogar die Datei-Struktur auf dem neuen (kopierten) Datenträger anders als beim Original sein. Aber in jedem Fall könnte der neue Datenträger nur Fehlermeldungen wie "Datei kann nicht geöffnet werden" oder "Datei nicht gefunden" oder "Datenfehler" hervorbringen. Das Test-/Scan-Programm (siehe Punkt 3 und 5) fragt aber nach genau den Fehlermel-

dungen, die nach physikalischer Beschädigung entstehen.

Es wird somit deutlich, daß nur derjenige, der die originalen Installations-Datenträger griffbereit hat, auch der einzige ist, der die betroffene Software dauerhaft nutzen kann. Im Gegensatz zur nachfolgenden Abwandlung kann der Besitzer die Software jedoch auf mehrere Computer in seinem Bereich oder Haus installieren. Manchmal ist dies gewünscht und seitens des Herstellers gebilligt. Es kann auch eine Art "Puffer" in das Test-Programm integriert werden, daß nicht bei der ersten Anforderung des Original-Installations-Datenträgers, dieser auch unbedingt eingelegt werden muß. Man könnte dem Anwender noch eine "zweite Chance" (oder natürlich auch dritte) geben.

Es wäre auch denkbar, daß bei der Installation der Software eine bestimmte Datei (oder mehrere Dateien, oder auch der gesamte Inhalt) auf dem veränderten Datenträger gelöscht oder verändert wird und diese Veränderung daßelbige Installationsprogramm bei dem nächsten Versuch die Software auf einem (wahrscheinlich anderen) Computer zu installieren, veranlaßt, keine weiteren Installationen durchzuführen. Aufgrund der Nicht-Kopierbarkeit der oder einer der Installations-Datenträger, wäre somit ausgeschlossen, daß wie momentan meist getan, die Installations-Datenträger vor der Installation kopiert werden und dann weitergegeben werden.

Ein Test-/Scan-Programm welches für Windows 3.x geschrieben wurde und dem Schutz von Computer-Software dient, kann vom Erfinder geliefert werden. Damit können diese speziellen Datenträger (bis auf die absichtliche Beschädigung) erzeugt dokumentiert und später auch getestet werden.

In naher Zukunft wird sicherlich die beschreibbare Compact-Disk (Nachfolger der heutigen CD, bzw. CD-Rom) in den Vordergrund treten. Sie wird vor allem die Videokassette (VHS, Video 2000, Beta, V8) ablösen und auch im sonstigen Multi-Media-Markt die Vorherrschaft erlangen. Gerade auf dem Videofilm-Sektor wird dadurch das bereits jetzt schon sehr große Problem der Raubkopien noch weiter ansteigen, da beim Kopieren keine Qualitätsverluste mehr entstehen.

Hier könnte beispielsweise ein mit auf der CD aufgebrachtes Testprogramm, vor dem Start des eigentlichen Videofilms, die CD — welche nach dem oben beschriebenen Verfahren behandelt wurde — auf Originalität testen. Nur bei erfolgreichem Test würde der Videofilm freigegeben. Aufgrund der vielen verschiedenen Formaten wird vielleicht auch das 'Abspielprogramm' bei einem Videofilm gleich mitgeliefert. Dies könnte dann das o.g. Testprogramm enthalten.

Patentansprüche

1. Verfahren zum Verhindern der Vervielfältigung von Software (Software-Kopierschutz) die auf einem Datenträgern aufgebracht bzw. mit/durch einem Datenträger geliefert wird, oder mit einem solchen in Verbindung steht bzw. abgesichert wird, **dadurch gekennzeichnet**, daß eine oder mehrere absichtlich erzeugte physikalische Beschädigung(en) oder Veränderung(en) des Datenträgers exakt in deren Auswirkungen auf vorher auf den Datenträger geschriebene/aufgebrachte Daten oder Dateien analysiert und das Ergebnis so dokumentiert/festgehalten/gespeichert wird, daß bei Anwendung der zu schützenden Software bzw. deren Installation eine oder die Software bzw. Programm oder auch eine elektronische Vorrichtung erneute Analysen dieses Datenträgers durchführt und das Ergebnis mit dem dokumentiertem Analyse-Ergebnis vergleicht um die Originalität des Datenträgers zu testen und dann dementsprechend zu reagieren.

2. Verfahren zum Verhindern der Vervielfältigung von Software (Software-Kopierschutz) die auf einem Datenträgern aufgebracht bzw. mit/durch einem Datenträger geliefert wird, oder mit einem solchen in Verbindung steht bzw. abgesichert wird, dadurch gekennzeichnet, daß eine oder mehrere nicht oder nur sehr unwahrscheinlich rekonstruierbare und/oder nicht oder nur sehr unwahrscheinlich kopierbare Veränderung(en)/Beschädigung(en) des Datenträgers so vorgenommen und dokumentiert werden, daß sie immer wieder (computer-)technisch nachgeprüft werden können.

3. Verfahren nach den Ansprüchen 1 und 2, dadurch gekennzeichnet, daß die Datenträger eine Diskette oder eine Compact-Disc in den verschiedensten Größen und Formaten (CD, SD, MOD, MD und alle zukünftig entwickelten Arten) sowie ein oder mehrmals beschreibbar und/oder löschbar sein kann. Es kommen auch Datenträger für Video, Audio, Multi-Media sowie deren Variationen, auch Streamer, Datenbänder, Kassetten und auch Festplatten in ihren jeweils unterschiedlichsten Variationen, in Betracht.

4. Verfahren nach den Ansprüchen 1 und 2, dadurch gekennzeichnet, daß die Veränderung(en) bzw. Beschädigung(en) durch einen oder mehrere Kratzer, Schnitt(e), Verformung(en), Wärmezufuhr bzw. -einwirkung(en), Laser-Einwirkung(-en), Farbe(n), Aufbringung weiterer Stoffe, chemische Veränderung(en) der Oberfläche(-n), magnetische Veränderung(en), Veränderung(en) der magnetischen oder sonstigen Eigenschaften, und/oder Veränderung(en) der optischen Eigenschaften, hinzufügen oder entfernen von Material(ien), entsteht.

5. Verfahren nach den Ansprüchen 1, 2 und 4, dadurch gekennzeichnet, daß die Veränderung(en) bzw. Beschädigung(en) dauerhaft/permanent und in gewissen Relationen — auch über längere Zeit — konstant sind.

6. Verfahren nach den Ansprüchen 1 und 2, dadurch gekennzeichnet, daß der Datenträger als erstes so mit Daten beschrieben wird, daß die nachfolgende Veränderung/Beschädigung gut lokalisiert/detektiert bzw. analysiert werden kann. Es kann auch nur ein bestimmter Teil/Bereich des Datenträgers zur Veränderung/Beschädigung bestimmt werden. Es können auch andere, verfahrensunabhängige Daten auf dem betroffenen Datenträger mit gespeichert werden, was jedoch zumeist auf einen Teilbereich des Datenträgers beschränkt sein wird, der nicht diesem Verfahren dient und somit weder mit den o.g. Daten beschrieben, noch nach den vorgenannten Ansprüchen beschädigt oder verändert wird.

7. Verfahren nach den Ansprüchen 1, 2 und 6, dadurch gekennzeichnet, daß die Daten (massenweise) kleine oder (wenige) große, einfache oder komplexe Dateien sind. Es können auch Blöcke, Sektoren, Spuren, oder sonstige bestimmte Bereiche/Teile des Datenträgers direkt beschrieben/geprägt/bedruckt/geätzt/gebrannt werden.

8. Verfahren nach den Ansprüchen 1 und 2, dadurch gekennzeichnet, daß die Veränderung(en) bzw. die Beschädigung(en) des Datenträgers und deren jeweilige Auswirkungen dadurch analysiert und erfaßt werden, daß die vorher aufgebrachten Daten (Anspruch 6 und 7) gelesen/getestet werden und entsprechende Abweichungen zu den ursprünglichen (vor Veränderung/Beschädigung) Sollwerten oder auftretende Probleme (durch eben dieses Analyse-Programm) genau festgehalten/dokumentiert werden.

9. Verfahren nach den Ansprüchen 1, 2 und 8, dadurch gekennzeichnet, daß die Dokumentation der Veränderung(en) bzw. das Ergebnis der Analyse nach der Beschädigung(en) des Datenträgers in einem oder dem zu schützenden Programm/Software, einer Datei, verschlüsselt auf dem oder einen anderen Datenträger, oder sonst kaum manipulierbarer "Stelle" unterzubringen um nicht zu sagen zu verstecken ist.

10. Verfahren nach den Ansprüchen 1 und 2, dadurch gekennzeichnet, daß der Datenträger dadurch immer wieder getestet werden kann, daß der Datenträger bzw. die auf ihn gespeicherten Daten in gleicher Weise analysiert bzw. gelesen/getestet werden, wie dies — wie in Anspruch 8 dargestellt — zur Dokumentation der Auswirkungen der absichtlichen Veränderung/Beschädigung auf die zuvor aufgebrachten Daten, geschah und diese aktuellen Analyse-Ergebnisse mit der o.g. Dokumentation (des allerersten Analyse-Ergebnisses) verglichen werden.

11. Verfahren nach den Ansprüchen 1, 2, 8, 9 und 10 dadurch gekennzeichnet, daß die Dokumentation (des allerersten Analyse-Ergebnisses) nach Anspruch 9 in ein oder das Programm/Unterprogramm der jeweiligen (zu schützenden) Software in Verbindung mit einem Test-Programm zum Testen des Datenträgers so untergebracht wird, daß dieses Test-Programm in bestimmten Zeitabschnitten und/oder per Zufall und/oder bei bestimmter Anwendungszeit/dauer und/oder bestimmter Anwendungsanzahl, oder einer Kombination dieser Maße, den veränderten/beschädigten Datenträger verlangt um ihn dann, wie in Anspruch 10 dargestellt, auf Echtheit zu testen. Das o.g. Testprogramm kann auch in einem Gerät/Laufwerk/Electronic untergebracht sein, oder von einer elektronischen Schaltung durchgeführt werden.

12. Verfahren nach den Ansprüchen 1, 2, 8, 9 und 10 dadurch gekennzeichnet, daß die Dokumentation nach Anspruch 9 in ein oder das Programm oder Teilprogramm oder Unterprogramm (vorzugsweise dem Installationsprogramm) der jeweiligen (zu schützenden) Software in Verbindung mit einem Test-Programm zum Testen des Datenträgers (nach Anspruch 10) so untergebracht wird, daß dieses Test-Programm bei der Installation den veränderten/beschädigten Datenträger verlangt um ihn dann auf Echtheit zu testen und einen Vermerk/eine Veränderung/Löschung auf diesem Datenträger herbeiführt, so daß dieses Test-Programm in Zukunft über die soeben erfolgte Installation informiert wird. Das o.g. Testprogramm kann auch in einem Gerät/Laufwerk/Electronic untergebracht sein, oder von einer elektronischen Schaltung durchgeführt werden. Somit kann die mehrmalige Installation des selben Programms unterbunden bzw. kontrolliert werden.

13. Verfahren nach den Ansprüchen 1 und 2 dadurch gekennzeichnet, daß die in Anspruch 10 dargestellte Analyse des Datenträgers durch ein Testprogramm erfolgt, welches als Teil- bzw. Unterprogramm des Hauptprogramms in der zu schützenden Software untergebracht, oder als gesondertes Programm von der zu schützenden Software aufgerufen wird, oder in dem Laufwerk zum Abspielen des Datenträgers, einem Zusatzgerät, dem Abspielgerät, Computer, oder sonst welcher elektronischen Einrichtung untergebracht bzw. durch sie ersetzt wird.

14. Verfahren nach den Ansprüchen 1 und 2 dadurch gekennzeichnet, daß bei einer nach Anspruch 10 festgestellten unzulässigen Abweichung des getesteten Datenträgers zum Original, die Anwendung bzw. die zu schützende Software blockiert, vernichtet, gesperrt, oder abgebrochen wird, oder die zu schützende Software nur bei Übereinstimmung des getesteten Datenträgers mit dem Original entschlüsselt wird, da sie nur in verschlüsselter Form vorliegt und ohne Entschlüsselung unbrauchbar ist, oder die zu schützende Software nur bei Übereinstimmung des getesteten Datenträgers mit dem Original geladen, gestartet oder abgespielt wird.